U.S. Department of Justice
Office of the Inspector General
Audit Division

Audit Report

Independent Evaluation Pursuant to the Government Information Security Reform Act Fiscal Year 2002

The Office of Justice Programs' Enterprise Network System

October 2002

03-01

INDEPENDENT EVALUATION PURSUANT TO THE GOVERNMENT INFORMATION SECURITY REFORM ACT FISCAL YEAR 2002

THE OFFICE OF JUSTICE PROGRAMS' ENTERPRISE NETWORK SYSTEM

OFFICE OF THE INSPECTOR GENERAL COMMENTARY AND SUMMARY

The Office of Justice Programs (OJP) is a federal agency within the Department of Justice (Department). Specifically, the OJP's mission is to develop the nation's capacity to prevent and control crime, improve the criminal and juvenile justice systems, increase knowledge about crime and related issues, and assist crime victims. The OJP's senior management team is comprised of the Assistant Attorney General (AAG), the Deputy Assistant Attorney General (DAAG), and five bureau heads.

The Enterprise Network System (ENS) is the overall general support system that provides enterprise-wide information infrastructure services in support of the OJP mission. The ENS provides storage, processing, and transmission of a large variety of the OJP accounting and administrative information. Mission and administrative support functions of the OJP rely extensively on the availability of the ENS and the access it provides to facilitate the OJP program participation and efficient financial management operations. All information on the ENS is considered sensitive but unclassified.

The Office of the Inspector General (OIG) selected the OJP as one of five sensitive but unclassified systems to review pursuant to the Government Information Security Reform Act (GISRA) for the fiscal year (FY) 2002. The OIG was required by GISRA to perform an independent evaluation of the Department's information security program and practices. This report contains the results of the ENS audit. Separate reports will be issued for each of the other systems evaluated pursuant to GISRA, including three systems that process classified information.

Under the direction of the OIG and in accordance with Government Auditing Standards, PricewaterhouseCoopers LLP (PwC) was selected to perform the ENS audit. The audit took place from May through July 2002 and consisted of interviews, on-site observations, and reviews of Department and component documentation to assess the ENS's compliance

with GISRA and related information security policies, procedures, standards, and guidelines.[1]

During our review of the ENS, KPMG LLP (KPMG) was performing an audit of the ENS security controls in support of the fiscal year 2002 financial statement audit. GISRA mandates (as part of the Paperwork Reduction Act) that the OIG and its contractors rely whenever possible on work performed by other reviewers for its GISRA audits, so as not to duplicate efforts. To avoid duplication, PwC limited its role to reviewing management and operational controls and relied on the testing of technical controls performed by KPMG.

PwC's testing did not identify any areas where additional work was required or where there appeared to be any inconsistency with the conclusions reached by KPMG. Therefore, for the vulnerabilities noted in this report, we[2] are not providing recommendations. Instead, we are consolidating and reporting the recommendations in the OIG's financial statement FY 2002 report to simplify tracking of recommendations and corrective actions.[3]

Based on PwC's and KPMG's assessments, we assessed management, operational, and technical controls at a medium to high risk to the protection of the ENS from unauthorized use, loss, or modification. Specifically, the auditors identified vulnerabilities in 7 of the 17 control areas. Two of the seven vulnerabilities were identified as high risks to the protection of the ENS as indicated in the following chart.

[1] In a September 1997 audit, report number 97-26, the OIG recommended that the Department develop effective computer security program guidance. The Department then revised its policy and released DOJ Order 2640.2D, "Information Technology Security," in July 2001, which was used in the analysis of this year's review.

[2] In this report, "we" refers either to the OIG or to PwC working under the direction of the OIG. With respect to the discussion of technical controls, "we" also encompasses the work performed by KPMG under the direction of the OIG.

[3] At the time of our audit, the financial statement audit report had not been issued.

CONTROL AREAS [4]	VULNERABILITIES NOTED
Management Controls	
1. Risk Management	
2. Review of Security Controls	
3. Life Cycle	√
4. Authorize Processing (Certification and Accreditation)	
5. System Security Plan	√
Operational Controls	
6. Personnel Security	√
7. Physical and Environmental Protection	
8. Production, Input/Output Controls	
9. Contingency Planning	√
10. Hardware and Systems Software Maintenance	
11. Data Integrity	
12. Documentation	
13. Security Awareness, Training, and Education	√
14. Incident Response Capability	
Technical Controls	
15. Identification and Authentication	√*
16. Logical Access Controls	√*
17. Audit Trails	

Source: The OIG's FY 2002 GISRA audit of ENS

√* Significant vulnerability in which risk was noted as high. A high-risk vulnerability is defined as one where extremely grave circumstances can occur by allowing a remote or local attacker to violate the security protection of a system through user or root account access, gaining complete control of a system and compromising critical information.

As a result of this audit, we identified the following vulnerabilities:

- Service request (SR) changes were made without proper management review.

[4] Control Areas as described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-26 "Security Self- Assessment Guide for Information Technology Systems."

- System security plans, operating procedure guides, the organizational chart, and system configuration management guides were not updated to reflect current conditions.

- User authentication policies and procedures were not effectively enforced.

- The contingency plan was not updated or tested.

- ENS personnel were not always trained on emergency procedures and the procedures were not always distributed to staff.

- Password security controls were not enforced because of ineffective communication of the OJP policies and procedures.

- Workstation area security was inadequate.

We concluded that these vulnerabilities occurred because the OJP management did not fully develop, enforce, or formalize agency-wide policies in accordance with current Department policies and procedures. Additionally, the Department did not enforce its security policies and procedures in the certification and accreditation process to ensure the ENS is protected from unauthorized use, loss, or modification. If not corrected, these security vulnerabilities threaten the ENS and its data with the potential for unauthorized use, loss, or modification.

TABLE OF CONTENTS

OBJECTIVE, SCOPE, AND METHODOLOGY

The fiscal year (FY) 2001 Defense Authorization Act (Public Law 106-398) includes Title X; subtitle G, "Government Information Security Reform Act" (GISRA). GISRA became effective on November 29, 2000, and amends the Paperwork Reduction Act of 1995 by enacting a new subchapter on "Information Security." It requires federal agencies to:

- Have an annual independent evaluation of their information security and practices performed.
- Ensure information security policies are founded on a continuous risk management cycle.
- Implement controls that assess information security risks.
- Promote continuing awareness of information security risks.
- Continually monitor and evaluate information security policy.
- Control effectiveness of information security practices.
- Provide a risk assessment and report on the security needs of the agencies' systems, and include the report in their budget request to the Office of Management and Budget (OMB).

The objective of the audit was to determine the U.S. Department of Justice's (Department) compliance with the GISRA requirements. The Enterprise Network System (ENS) was selected as one of the subset of systems to be tested to determine the effectiveness of the Department's overall security program for FY 2002. At the time of our audit, KPMG LLP (KPMG) was performing a significant portion of the information security work required by GISRA as part of the Department's financial statement audits. KPMG was contracted to perform this work under the supervision of the OIG.

In determining if the Department is compliant with GISRA requirements, we used the collective work of both KPMG and PricewaterhouseCoopers LLP (PwC) to determine whether adequate computer security controls existed to protect the ENS from unauthorized use, loss, or modification. Although this report contains security vulnerabilities, we are not prescribing recommendations. Instead, we are consolidating and reporting the recommendations in the OIG's financial statement FY 2002 report to simplify tracking of recommendations and corrective actions.

We interviewed the OJP management personnel, reviewed system documentation, and performed testing to determine compliance with the Office of Justice Programs (OJP) and Department security policies and procedures. We performed the audit in accordance with Government Auditing Standards and the audits took place from May through July 2002. We performed test work at the OJP Headquarters in Washington, D.C.

For the interviews conducted, we used the questionnaire contained in the National Institute of Standards and Technology (NIST) Special Publication 800-26 "Security Self-Assessment Guide for Information Technology Systems." This questionnaire contains specific control objectives and suggested techniques against which the security of a system or group of interconnected systems can be measured. The questionnaire contains 17 areas under 3 general controls (management, operational, and technical). The areas contain 36 critical elements and 225 supporting security control objectives and techniques (questions) about the system. The critical elements are derived primarily from OMB Circular A-130 and are integral to an effective IT security program. The control objectives and techniques support the critical elements. If a number of the control objectives and techniques are not implemented, the critical elements have not been met.

The audit approach was based on the General Accounting Office's Federal Information System Controls Audit Manual, the Chief Information Officer Council Framework, OMB Circular A-130, and guidance established by NIST. These authorities prescribe a review that evaluates the adequacy of management, operational, and technical controls over control areas listed in Appendix I.

ENTERPRISE NETWORK SYSTEM (ENS) ENVIRONMENT

The OJP's Corporate Network, also known as the ENS, was selected by the OIG in consultation with Department management as one of the subset of systems to be tested to determine the effectiveness of the Department's overall security program for FY 2002. The ENS supports the information processing needs of more than 800 OJP employees and over 600 contract employees. The ENS network is a client/server network, and consists of a variety of network platforms including Novell Netware, Windows NT, and UNIX.

The ENS infrastructure consists of the Private Network and the Public Services Network. The Private Network provides maximum security safeguards for the OJP's most valuable systems and services by providing access only to OJP personnel. The Public Services Network provides

restricted interoperability with the public through significant security safeguards.

The ENS is physically housed in Washington, D.C., and is the general support system that provides enterprise-wide communication infrastructure services in support of the OJP mission. The information stored, processed, and transmitted on the ENS is sensitive but unclassified (SBU) information. The ENS contains government business and financial information that, if disclosed to unauthorized sources, could result in financial loss or adverse legal actions to the OJP.

SUMMARY RESULTS OF THE AUDIT

We obtained audit evidence to determine whether adequate computer security controls existed to protect the OJP network from unauthorized use, loss, or modification. We assessed management, operational, and technical controls for 17 critical areas as a medium to high risk for the ENS. Our assessment disclosed vulnerabilities within 7 of the 17 areas. Two of the seven vulnerabilities were within technical controls and were identified as high risks to the protection of the OJP network. For the vulnerabilities noted in this report, we are not providing recommendations. Instead, we will consolidate and report the recommendations in the OIG's financial statement FY 2002 report to simplify tracking of recommendations and corrective actions.

We concluded that these vulnerabilities occurred because the OJP management did not fully develop, enforce, or formalize agency-wide policies in accordance with current Department policies and procedures. Additionally, the Department did not enforce its security policies and procedures in the Certification and Accreditation process to ensure the ENS network was protected from unauthorized use, loss, or modification. If not corrected, these security vulnerabilities threaten the ENS and its data with the potential for unauthorized use, loss, or modification.

FINDINGS

Our review disclosed that security controls need improvement to fully protect the ENS from unauthorized use, loss, or modification. Specifically, vulnerabilities were identified in the following areas: life cycle controls; system security planning; personnel security; security awareness, training, and education; contingency planning; identification and authentication; and logical access controls. These vulnerabilities occurred because the OJP management did not enforce or formalize agency-wide and Department-level policies and procedures to fully secure the system.

I. Management Controls. Management controls are techniques and concerns that are normally addressed by management in the organization's computer security program. In general, they focus on the management of the computer security program and the risk within the organization.

Management Controls	Vulnerabilities Noted
Risk Management	
Review of Security Controls	
Life Cycle	√
Authorize Processing (Certification and Accreditation)	
System Security Plan	√

Our testing confirmed that management controls were adequate in the areas of risk management, review of security controls, and authorize processing. However, we found vulnerabilities in the following management control areas:

A. Life Cycle. Security is an important part of the system life cycle, and security is best managed if planned for the entire system life cycle. There are many models for the system life cycle, but most contain five basic phases: initiation, development/acquisition, implementation, operation, and disposal.

Issue: Service Request

Condition:

We found that the only service request (SR) change submitted during the FY was moved into production without appropriate approval from the Configuration Management manager. In addition, the OJP staff does not follow the OJP's configuration management policies on approval signatures.

Cause:

The OJP staff does not consider this signature a priority and does not enforce the requirement because other signatures (such as a requester's supervisor's signature and completion signature) are required and obtained before changes are moved into production.

Criteria:

The "OJP System Configuration Management Guide," dated November 12, 1999, requires the Configuration Management manager's approval for software changes.

Risk:

Without the appropriate approval signatures, code may enter the production environment without proper management review. This increases the risk that code may malfunction or cause damage to the OJP systems or information in the production environment.

B. System Security Plan. A system security plan provides an overview of the security requirements of the system and describes the controls in place or planned for meeting those requirements. The plan delineates responsibilities and expected behavior of all individuals who access the system.

Issue: Outdated Documentation

Condition:

The ENS system security plan, operating procedure guides, the organizational chart, and system configuration management guides have not been updated since December 15, 2000, to reflect current conditions at the OJP for FY 2002. The OJP policies, procedures, and guides refer to the Information Resource Management Division (IRMD) rather than the newly formed Office of the Chief Information Officer.

Cause:

The re-organizational change from the IRMD to the Office of the Chief Information Officer has not been incorporated in the OJP's official documents.

Criteria:

NIST Special Publication (SP) 800-18, "Guide for Developing Security Plans for Information Technology Systems," *Section 3.2.2 – Responsible Organization,* requires that the OJP "list the federal organizational sub-component responsible for the system."

NIST SP 800-18, *Section 3.2.4 – Assignment of Security Responsibility,* states: "an individual must be assigned responsibility in writing to ensure that the application or general support system has adequate security."

Risk:

Outdated documentation could lead to confusion as to the current status and responsibilities of key individuals at the OJP.

II. Operational Controls. Operational controls address security controls that are implemented and executed by people. These controls are put in place to improve the security of a particular system. They often require technical or specialized expertise and rely upon management activities as well as technical controls.

Operational Controls	Vulnerabilities Noted
Personnel Security	√
Physical and Environmental Protection	
Production, Input/Output Controls	
Contingency Planning	√
Hardware and Systems Software Maintenance	
Data Integrity	
Documentation	
Security Awareness, Training, and Education	√
Incident Response Capability	

Our testing confirmed that operational controls were adequate within the areas of physical and environmental protection; production, input/output controls; hardware and systems software maintenance; data integrity; documentation; and incident response capability. However, our testing identified vulnerabilities within other critical areas of operational controls. The specific details of the identified vulnerabilities are listed below.

A. Personnel Security. Personnel security involves the use of computer systems by human users, designers, implementers, and managers. A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their jobs.

Issue: Policy and Procedures

Condition:

Documentation to support compliance with the OJP remote user authorization policies and procedures does not exist. Specifically, we noted the following weaknesses:

- Two out of 15 users did not have documentation on file supporting the approval of access to related OJP systems;

- Nine out of 15 remote users have not signed the "Secure-UserID" form required by the OJP for remote user authorization; and

- Three out of 15 users did not have documentation on file supporting their termination from related OJP systems.

Cause:

The policies and procedures within the OJP Security Operating Procedures Guide (SOPG) have not been enforced. Specifically, methods unrelated to policy are used by the OJP management to expedite their user authentication. For example, e-mail or verbal confirmation have been used rather than methods compliant with the policies set forth by the OJP SOPG.

Criteria:

"Office of Justice Programs, Security Operating Procedures Guide (SOPG)," *Section 3.1.1 – User Account Authorization,* requires the following:

- Requests for dial-in access will be submitted, in writing, to the Computer System Security Officer (CSSO) and have approval from the Bureau/Office head.

- Authorized users will receive a SecureID key from the contractor.

- Users must sign a SecureID receipt and are responsible for safeguarding the SecureID key.

- Users must attend one-on-one orientation with the Network Communications Administrator.

Risk:

Without effective enforcement of user authentication policies and procedures, the authorization process may be circumvented, resulting in an individual obtaining remote access without proper authorization or justification.

B. Contingency Planning. Contingency planning ensures continued operations by minimizing the risk of events that could disrupt normal operations and having an approach in place to respond to those events should they occur.

Issue: Backup and Service Continuity

Condition:

The following weaknesses were identified to the OJP's backup and service continuity procedures:

- Oracle backup tapes are not sent to the off-site facility on a weekly or bi-weekly basis.

- The contingency plan does not call for a backup site.

- Performance goals have not been established for server availability therefore causing contractors to overlook server availability.

Cause:

The Oracle contractors are not following the OJP procedure to ship backup tapes to the off-site facility either weekly or bi-weekly. The Office of the Chief Information Officer has not recognized the need to provide server availability goals for the contractors responsible for maintaining server availability. In addition, the contractors do not monitor server availability on a long-term basis, since they do not have formal guidelines from the OJP on the acceptable level of downtime.

Criteria:

OJP's Automated Information System Security Plan for the Enterprise Network System, dated December 15, 2000, *Section 4.4 - Contingency Planning,* requires that at the end of the week, all incremental tapes and the full (weekly) backup tape be stored off-site.

Risk:

Backup tapes of critical Oracle data may be lost in the event that a disaster occurs at the OJP facility. In the event that the OJP loses its on-site data from the Oracle servers, the OJP would not be able to replace valuable information.

Because server availability is not monitored adequately, the contractors and the OJP staff might not recognize a long-term degradation in server performance levels in time to effectively address the problem.

Issue: Contingency Plan

Condition:

- The plan has not been updated since FY 2000.
- OJP staff have not been trained on the plan nor has the plan been distributed to the staff.
- The plan does not specify the length of time before operations should resume.
- The plan does not have formal test procedures or polices in place for testing.

Cause:

According to OJP management, the Office of the Chief Information Officer has not had the resources (staff and budget) to update the contingency plan since FY 2000. The Office of the Chief Information Officer does not see the benefit in distributing the existing plan due to its length. Thus, staff were not trained on the current contingency plan. Additionally, the contingency plan does not establish specific timelines because the developers of the plan wanted to keep the plan vague. Finally, the Office of the Chief Information Officer believes that occasional accidents, such as server outages or inclement weather problems, serve as the test of the contingency plan. The Office of the Chief Information Officer does not perform additional tests of the contingency plan.

Criteria:

OMB Circular A-130, Appendix III, *Security of Federal Automated Information Systems*, states: "Agency plans should assure that there is an ability to recover and provide service sufficient to meet the minimal needs of users of the system."

NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, *Section 3.6.5 – Test and Revise Plan,* requires that an organization test and revise the contingency plan. Additionally, NIST requires that the organization update the plan since it will become outdated as time passes and as the resources used to support critical functions change.

DOJ Order 2640.2D, *Information Technology Security*, *Chapter 1, Section 9, Contingency Planning/Business Resumption Planning* requires components test contingency/business resumption plans annually or as soon as possible after a significant change to the environment that would alter the in-place assessed risk.

NIST SP 800-12, Section 11 – *Preparing for Contingencies and Disasters* states: "Contingency planning involves more than planning for a move offsite after a disaster destroys a data center. It also addresses how to keep an organization's critical functions operating in the event of disruptions, both large and small. This broader perspective on contingency planning is based on the distribution of computer support throughout an organization."

NIST SP 800-14, *Section 3.6.2 – Identify Resources,* states: "Time Frame Needed. In addition, an organization should identify the time frames in which each resource is used and the effect on the mission or business of the continued unavailability of the resource."

Risk:

During an extended outage and/or disaster, information system processing functions and vital business operations may be damaged and unable to function. Without a comprehensive business continuity plan, the OJP could face potentially critical financial data losses in the event of a disaster. Testing is one of the most important functions in maintaining a viable disaster recovery plan. It is through testing that weaknesses in the plan are uncovered and can be corrected. Testing should be performed to ensure that critical information for continued operations is not lost due to a failure to fully identify information technology recovery needs during a disaster.

C. Security Awareness, Training, and Education. People are a crucial factor in ensuring the security of computer systems and valuable information resources. Security awareness, training, and education enhance security by improving awareness of the need to protect system resources. Additionally, training develops skills and knowledge so computer users can perform their jobs more securely.

Issue: Emergency Procedures

Condition:

From interviews with the OJP management and staff regarding the OJP's emergency procedures, we noted the following:

- Staff members have not been trained on emergency procedures.
- Emergency procedures have not been distributed to the staff.

Cause:

The Office of Administration considers the bi-annual fire drills adequate training on emergency procedures. Key individuals are trained monitors for each floor and are responsible for ensuring that everyone is evacuated in the event of an emergency. According to the OJP management, the Emergency Operations and Occupation Plan are not distributed because the document is too large.

Criteria:

OMB Circular A-130, states that management should plan for how they will perform their mission and/or recover from the loss of existing application support, whether the loss is due to the inability of the application to function or a general support system failure.

NIST SP 800-12, S*ection 11 – Preparing for Contingencies and Disasters* states: "Contingency planning involves more than planning for a move offsite after a disaster destroys a data center. It also addresses how to keep an organization's critical functions operating in the event of disruptions, both large and small. This broader perspective on contingency planning is based on the distribution of computer support throughout an organization."

Risk:

Without proper training employees may not be adequately prepared to respond appropriately in the event of an emergency.

III. Technical Controls. Technical controls focus on security controls that the computer system executes and depend upon the proper functioning of the system to be effective. Technical controls require significant operational considerations and should be consistent with the management of security within the organization.

Technical Controls	Vulnerabilities Noted
Identification and Authentication	√*
Logical Access Controls	√*
Audit Trails	

√*Significant vulnerability in which risk was noted as high. A high-risk vulnerability is defined as one where extremely grave circumstances can occur by allowing a remote or local attacker to violate the security protection of a system through user or root account access, gaining complete control of a system and compromising critical information.

During our review of the ENS, KPMG was performing an audit of the ENS security controls in support of the FY 2002 financial statement audit. KPMG assessed the technical controls using commercial-off-the-shelf and proprietary software to conduct network scanning on the ENS. The technical vulnerabilities reported in this report are KPMG's results relied upon by PwC.

As a result of testing ENS's technical controls, we confirmed that controls were adequate in the areas of audit trails. Test results identified high vulnerabilities within critical areas of ENS's technical controls as listed below.

A. Identification and Authentication. Identification and authentication are technical measures that prevent unauthorized people or processes from entering an IT system. Identification, most commonly used for access control, is the means by which users claim their identities to a system. Authentication is the verification that a person's claimed identity is valid and is usually implemented through the use of passwords.

A password is a unique string of characters that must be provided before a logon or access is authorized to a computer system. Passwords are security measures used to restrict logons to user accounts and access to computer systems and resources. The OJP password controls tested via network security penetration testing were found to be inadequate.

Issue: Authentication Controls

Condition:

User authentication controls are not in compliance with policies and procedures set forth by the OJP password management guidelines. Specifically, we noted the following instances of weak or non-existent passwords in place on key business database servers, operating system accounts, and network devices:

- Null session connections to the OJP registered Primary Domain Controller.
- Default database server account/passwords.
- Passwords equal to user name.
- Blank passwords.
- Default Simple Network Management Protocol (SNMP) community strings on network devices.

Cause:

Ineffective communication of the OJP policies and procedures to administrative staff has created a situation where password security controls are not enforced. Specifically, we noted numerous instances where administrators were not aware of the password guidance provided by the OJP Computer Security Program.

Criteria:

Department of Justice – Office of Justice Programs: Computer System Password Policy, Section 3, requires that passwords will be used on all automated information systems to protect systems and system level accounts, individual accounts, and sensitive information processed or stored by the systems.

- All user and system passwords should be at least eight characters in length.

- All user and system passwords should consist of a mix of at least three of the following: English uppercase, English lower case, numeric, special characters.

- Dictionary words, simple keyboard patterns, or character strings, shall not be used.

DOJ Order 2640.2D, "Information Technology Security" Chapter *2, Section 18*, requires that Department IT systems that use passwords as the means for authentication shall implement at least the following minimum features:

- An eight-character password composed of at least three of the following: English uppercase, English lower case, numeric, and special characters.

- Prevent the use of previous six passwords.

- Prevent the display of a clear text password.

- Limit password lifetime to a maximum of ninety (90) days.

Furthermore, DOJ Order 2640.2D, Chapter *2, Section 18,* states Department IT systems shall: "disable system default passwords as soon as possible after system installation and before the system becomes operational."

Risk:

Poor password security parameters subject critical ENS information to potential unauthorized accessed and prevent the ENS system administrators from detecting unauthorized access on a system. Easily guessed passwords obtained during a brute force attack may compromise the identification and authentication integrity of the ENS servers.

B. Logical Access Controls. Logical access controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted.

Issue: Network Devices

Condition:

The OJP did not enforce technical controls to achieve optimal workstation security resulting in the use of unauthorized network devices within the OJP facility. Specifically, we found:

- Active network ports in vacant cubicles.
- No password-protected screensavers for unattended terminals.
- Warning banners not displayed upon login.

Cause:

Controls to enforce workstation security, as specified in the OJP SOPG, have not been effectively communicated to OJP system users. For example, the Dynamic Host Configuration Protocol (DHCP) server responds to DHCP client requests; however, an unattended workstation with an active drop can be used by any user and computer recognized by the network servers.

Criteria:

"Department of Justice – Office of Justice Programs: Enterprise Security Network Security Operating Procedures Guide (SOPG)," S*ection 4.7.4 – Workstation Area Security,* requires the following:

- Access controls must be enabled to provide security to limit access to only authorized individuals.
- Users must ensure a screen saver is enabled with password protection when leaving their workstation for a period of time.

DOJ Order 2640.2D, "Information Technology Security," Ch*apter 2, Section 20 - Warning Banner,* requires "all Department IT systems implement a system banner that provides warnings: to employees that accessing the system constitutes consent to system monitoring for law enforcement and other purposes; and to unauthorized users that their use of the system may subject them to criminal prosecution and/or criminal or civil penalties."

Risk:

Inadequate workstation area security may allow an unauthorized user to use an unattended workstation to gain access to network resources by allowing the unauthorized user to view sensitive data that was not properly secured using a screen saver. In addition, unauthorized full network access may be gained by connecting a computer directly to an active network drop.

Issue: Denial of Service

Condition:

We used an automated vulnerability scanner, NESSUS, to detect possible exploitable weaknesses associated with the OJP's public web servers. We noted that one web server is vulnerable to a possible "denial-of-service" (DOS) attack, and one web server discloses various parts of its directory structure. A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include, attempts to "flood" a network, thereby preventing legitimate network traffic, and attempts to disrupt connections between two machines, thereby preventing access to a service.

Cause:

The identified web servers have not been updated to address the latest vulnerabilities.

Criteria:

OMB Circular A-130, Appendix III, *"Security of Federal Automated Information Resources,"* states: "in every general support system, a number of technical, operational, and management controls are used to prevent and detect harm. Such controls include individual accountability, "least privilege," and separation of duties.

Individual accountability consists of holding someone responsible for his/her actions. In a general support system, accountability is normally accomplished by identifying and authenticating users of the system and subsequently tracing actions on the system to the user who initiated them. Least privilege is the practice of restricting a user's access (to data files, to processing capability, or to peripherals) or type of access (read, write, execute, delete) to the minimum necessary to perform his job."

Risk:

The current vulnerabilities allow an attacker to perform DOS attacks that could potentially shut down the ENS web server. Additionally, by requesting the "robot.txt" file, the attacker can ascertain the directory structure on the web server and modify information.

CONCLUSION

Our review disclosed that security controls need improvement to fully protect the ENS from unauthorized use, loss, or modification. Specifically, we found vulnerabilities in the areas of life cycle controls, system security planning; personnel security; contingency planning; security awareness, training, and education; identification and authentication; and logical access controls. We assessed these vulnerabilities as a medium to high risk to the ENS. If not corrected, these security vulnerabilities threaten the data stored on the ENS with the potential for unauthorized use, loss, or modification.

APPENDIX I

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY GENERAL CONTROL AREAS

The review focused on evaluating the adequacy of management, operational, and technical controls over the following specific control areas:

I. MANAGEMENT CONTROLS. Management controls focus on the management of the IT security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management.

- **Risk Management**. Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. Assessing risk management involves evaluating OJP's efforts to complete the following critical procedures:

    - Periodic performance of a system risk assessment had been performed.
    - Program officials understand the risk to systems under their control and had determined the acceptable level of risk.

- **Review of Security Controls.** Routine evaluations and response to identified vulnerabilities are important elements of managing security controls of a system. Determining whether review of security controls had been adequately performed requires the auditor to assess if the following critical items were completed:

    - A system security control review had been performed for both the ENS and interconnected systems.
    - Management ensured effective implementation of corrective actions.

- **Life Cycle.** Like other aspects of an IT system, security is best managed if planned for throughout the IT system life cycle. There are many models for the IT system life cycle but most contain five basic phases: initiation, development/acquisition, implementation, operation, and disposal. Assessing a system's life cycle involves identifying if the following critical items are in place for the ENS:

    - A system development life cycle methodology.

- System change controls as programs progress through testing to final approval.

- **Authorize Processing (Certification and Accreditation).** Authorize processing (also referred to as certification and accreditation) provides a form of assurance of the security of the system. To determine whether the ENS had been appropriately authorized to process data involves analyzing critical documents that identify whether:

  - The system had been certified/recertified and authorized to process (accredited).
  - The system is operating on an interim authority in accordance with specified agency procedures.

- **System Security Plan.** A system security plan provides an overview of the security requirements of the system and describes the controls in place or planned for meeting those requirements. The plan delineates responsibilities and expected behavior of all individuals who access the system. Assessing whether the ENS has an adequate system security plan requires identifying if the following critical elements were met:

  - A system security plan had been documented for the system and all interconnected systems if the boundary controls are ineffective.
  - The plan is kept current.

II. OPERATIONAL CONTROLS. Operational controls address security controls that are implemented and executed by people. These controls are put in place to improve the security of a particular system. They often require technical or specialized expertise and rely upon management activities as well as technical controls.

- **Personnel Security.** Many important issues in computer security involve human users, designers, implementers, and managers. A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their jobs. Assessing personnel security involves evaluating the OJP efforts to complete the following critical procedures:

  - Duties are separated to ensure least privilege and individual accountability.

- Appropriate background screening is completed.

- **Physical and Environmental Protection.** Physical security and environmental security are the measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. Assessing physical and environmental protection involves evaluating OJP's efforts to complete the following critical procedures:

  - Adequate physical security controls have been implemented and are commensurate with the risks of physical damage or access.
  - Data is protected from interception.
  - Mobile and portable systems are protected.

- **Production, Input/Output Controls.** There are many aspects to supporting IT operations. Topics range from a user help desk to procedures for storing, handling and destroying media. Assessing production, input/output controls involves evaluating the OJP efforts to complete the following critical procedures:

  - User support is being provided to ENS users.
  - Media controls are in place for the ENS.

- **Contingency Planning.** Contingency planning ensures continued operations by minimizing the risk of events that could disrupt normal operations and having an approach in place to respond to those events should they occur. Assessing contingency planning involves evaluating OJP's efforts to complete the following critical procedures:

  - Identify the most critical and sensitive operations and their supporting computer resources.
  - Develop and document a comprehensive contingency plan.
  - Have tested contingency/disaster recovery plans in place.

- **Hardware and System Software Maintenance**. These are controls used to monitor the installation of, and updates to, hardware and software to ensure that the system functions as expected and that a historical record is maintained of changes. Some of these controls are also covered in the Life Cycle Section. Assessing hardware and system software maintenance involves evaluating OJP's efforts to complete the following critical procedures:

- Access is limited to system software and hardware.
- All new and revised hardware and software are authorized, tested, and approved before implementation.
- Systems are managed to reduce vulnerabilities.

- **Data Integrity.** Data integrity controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets expectations about its quality and integrity. Assessing data integrity involves evaluating OJP's efforts to complete the following critical procedures:

  - Virus detection and elimination software is installed and activated.
  - Data integrity and validation controls are used to provide assurance that the information has not been altered and the system functions as intended.

- **Documentation.** The documentation contains descriptions of the hardware, software, policies, standards, procedures, and approvals related to the system and formalize the system's security controls. Assessing documentation involves evaluating OJP's efforts to complete the following critical procedures:

  - There is sufficient documentation that explains how software/hardware is to be used.
  - There are documented formal security and operational procedures.

- **Security Awareness, Training, and Education.** People are a crucial factor in ensuring the security of computer systems and valuable information resources. Security awareness, training, and education enhance security by improving awareness of the need to protect system resources. Additionally, training develops skills and knowledge so computer users can perform their jobs more securely and builds in-depth knowledge. Assessing security awareness, training, and education involves evaluating OJP's efforts to complete the following critical procedures:

  - Employees have received adequate training to fulfill their security responsibilities.

- **Incident Response Capability.** Computer security incidents are an adverse event in a computer system or network. Such incidents are becoming more common and their impact is far-reaching. The following questions are organized according to two critical elements. Assessing incident response capability involves evaluating OJP's efforts to complete the following critical procedures:

    - There is a capability to provide help to users when a security incident occurs in the system.
    - Incident-related information is shared with appropriate organizations.

III. TECHNICAL CONTROLS. Technical controls focus on security controls that the computer system executes and depend upon the proper functioning of the system to be effective. Technical controls require significant operational considerations and should be consistent with the management of security within the organization.

- **Identification and Authentication.** Identification and authentication is a technical measure that prevents unauthorized people or processes from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users. Authentication is verification that a person's claimed identity is valid and it is usually implemented through the use of passwords. Assessing identification and authentication involves evaluating OJP's efforts to complete the following critical procedures:

    - Users are individually authenticated via passwords and other devices.
    - Access controls are enforcing segregation of duties.

- **Logical Access Controls.** Logical access controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted. Assessing logical access controls involves evaluating OJP's efforts to complete the following critical procedures:

    - Logical access controls restrict users to authorized transactions and functions.
    - There are logical controls over network access.

- There are controls implemented to protect the integrity of the application and the confidence of the public when the public accesses the system.

- **Audit Trails**. Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide individual accountability, a means to reconstruct events, detect intrusions, and identify problems. Assessing audit trails involves evaluating OJP's efforts to complete the following critical procedures:

  - Activity involving access to and modification of sensitive or critical files is logged, monitored, and possible security violations are investigated.

APPENDIX II

REPORT STATUS

For the vulnerabilities noted in this report, as previously discussed, we are not providing separate recommendations. Instead, we will consolidate and report the recommendations in the OIG's financial statement FY 2002 report to simplify tracking of recommendations and corrective actions. Therefore, this report is closed.